



Projeto de Formatura – 2023 – Press Release

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema: Machine Learning aplicada a segurança em Internet das Coisas: detectando anomalias na comunicação e operação.

Considerando a interconexão expansiva e a proliferação de dispositivos inteligentes em nossa vida cotidiana, a segurança na Internet das Coisas (IoT) se torna uma prioridade crítica. A natureza simples e muitas vezes vulnerável desses dispositivos apresenta um cenário propício para potenciais ameaças cibernéticas, colocando em risco informações sensíveis e a funcionalidade desses sistemas.

Os Sistemas de Detecção de Intrusão (IDS) assumem um papel fundamental, monitorando constantemente o tráfego de rede em busca de atividades suspeitas ou anômalas. Esses sistemas identificam padrões incomuns e comportamentos maliciosos, permitindo uma resposta rápida e proativa para mitigar possíveis ataques, fortalecendo assim a integridade e segurança dos dispositivos IoT. Um IDS desenvolvido por um aluno de graduação da Escola Politécnica da USP apresenta uma solução de um sistema que alia informações de operação dos sensores e as métricas da rede que eles estão inseridos. Isto oferece, diz o aluno, “uma solução com mais ferramentas para monitorar e proteger as redes de dispositivos IoT”.

A detecção de intrusão utiliza de inteligência artificial para classificar a rede em normal ou anômala. Ela é treinada por muitos dados coletados por horas de simulações e assimila o que é um comportamento “normal” da rede. Quando as métricas fogem do padrão, o sistema a classifica como anômala e apresenta ao usuário que pode estar ocorrendo um ataque.

A acurácia do modelo é de 96% e o sistema é capaz de detectar uma intrusão em até um minuto depois que o ataque começa. Mas até chegar nestes resultados, o aluno realizou a simulação de uma rede padrão em emuladores de rede voltados à IoT. Também implementou três ataques diferentes para a construção de um banco de dados que veio então a ser utilizado para realizar o treinamento do sistema. A pesquisa realizada na Escola Politécnica evidencia um compromisso crescente da área de engenharia de computação no desenvolvimento da temática de cybersegurança. Os resultados apresentam o impacto positivo de alinhar diferentes temas de pesquisa, neste caso Segurança e Inteligência Artificial, para construir soluções cada vez melhores.

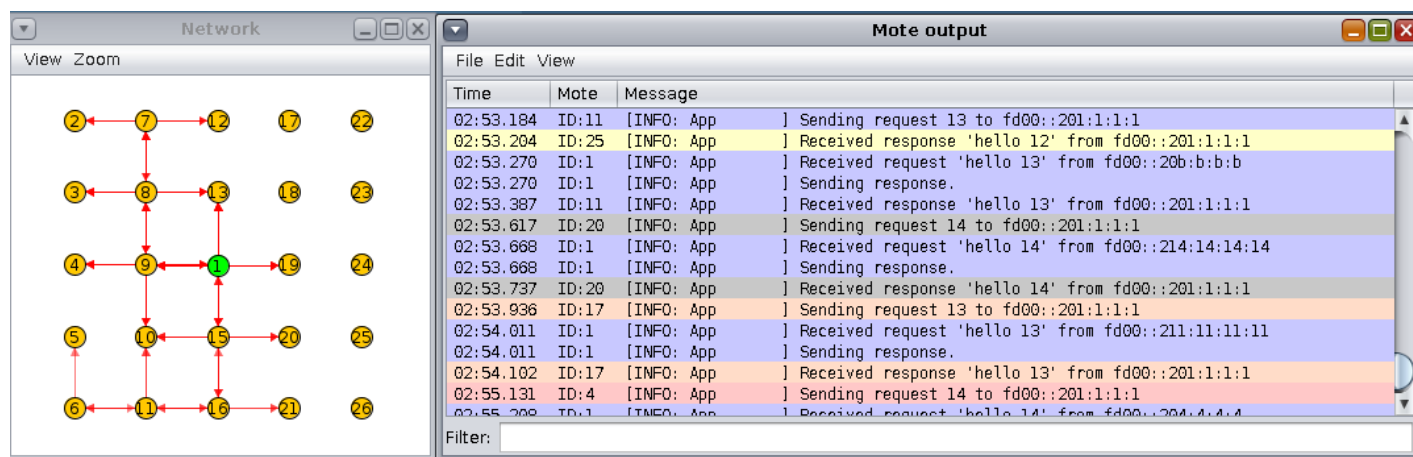


Figura 1: Simulação no Contiki Cooja, emulador utilizado para a coleta dos dados da Pesquisa.

Integrante: Alexandre Marques Carrer

Professora Orientadora: Cíntia Borges Margi
Co-orientador: Artur Jordão Lima Correia